

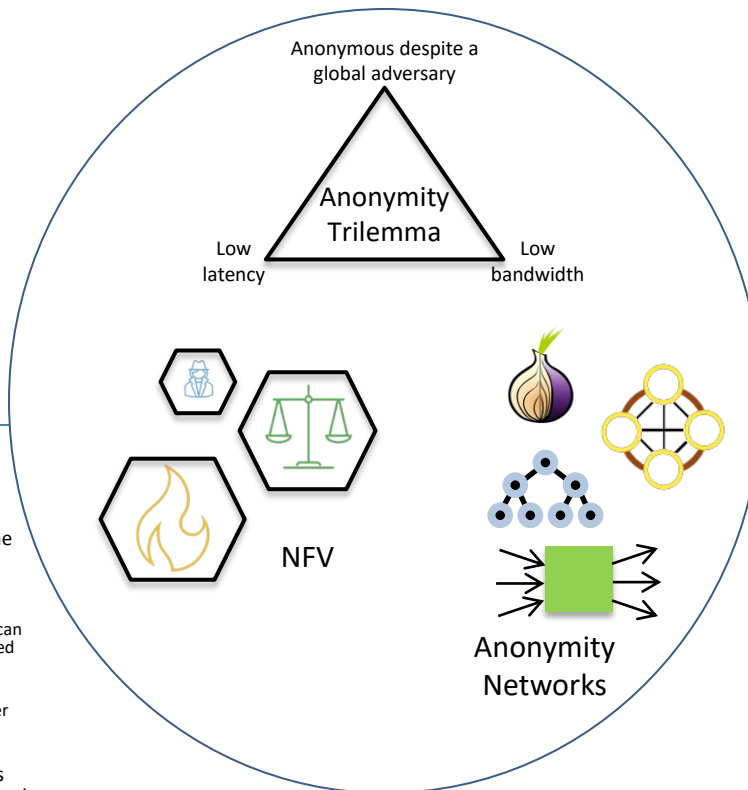
# Building Sophisticated Services with Programmable Anonymity Networks

## Challenge:

- Difficult to deploy new services in anonymity networks or react to new attacks.
- Anonymity systems must make a fundamental trade-off referred to as the “anonymity trilemma”: no one system can simultaneously achieve strong anonymity, low latency, and high bandwidth.
- While all three properties may not be simultaneously achievable, a more programmable anonymity network can let users choose their precise set of trade-offs and deploy new functionality.
- However, we then operate within a threat model that prior NFV work has not explored: one in which the client and middlebox are mutually distrusting.
- This leads to new concerns that must be addressed to allow one to safely and securely deploy NFV-like functionality in anonymity networks.

## Solution:

- By using recent advances in trusted execution environments (conclaves), Bento ensures that the client is protected from the middlebox, and the middlebox is protected from the client.
- Bento consists of four broad parts:
  - User-written and provided functions that they can run and interact with on specific Tor relays called Bento servers.
  - An execution environment for these functions.
  - A policy enforcement layer to exert control over what functions can do.
  - The resources that functions need to access.
- Functions run in trusted execution environments and they forward all calls to the policy enforcement layer, which decides whether or not to give them access to resources. This allow us to achieve programmability in anonymity networks safely and securely.



## Scientific Impact:

- Tor has become a staple in resisting censorship and allowing journalists to safely communicate with their sources.
- We introduce Bento, the first architecture to safely bring the power of NFV to anonymity networks like Tor.
- We identify, design, and implement critical components that are necessary to ensure expressiveness and safety of an anonymous middlebox architecture.
- We present middlebox functions that solve a wide diversity of problems that have long plagued the Tor network, including website fingerprinting defenses and more robust hidden services.

## Broader Impact and Broader Participation:

- Anonymity systems are critical in achieving free, open communication on today's Internet.
- Improve the security, agility, and evolvability of anonymity networks.
- 10+ undergrads obtained their first research experiences, multiple masters and PhD students funded.
- Open source code, artifact evaluated code